REMARKS/ARGUMENTS

Applicant has amended his claims to overcome the "indefiniteness" objections and rejections. Applicant has also added a new independent claim 154 that includes similar limitations to claim 1 but omits the "consisting essentially of" language of the claim 1 claim preamble. Applicants request the Examiner to reconsider and allow this application in view of the proposed amendments and the following remarks.

The Examiner withdrew his previous rejection based on Bellovin, but now rejects all claims as "obvious" in view of Vanstone combined with Bellovin together or with Wu. However, as will be explained below, adding ideas to Vanstone from Bellovin has relatively limited effect. Applicant respectfully submits that the methods disclosed and claimed herein are more elegant, less computationally intensive, as secure or more so, and better suited to real-world mobile uses than the method disclosed by Vanstone (with or without Bellovin combinations).

Vanstone's disclosed process involves two public-private key pairs, generation of three random numbers, two Diffie-Hellman calculations, two SHA hashes, and a digital signature. For example, Vanstone's rather complex and involved protocol appears to require the calling party (the client) to:

- generate two random numbers,
- store a public-private key pair on disk,
- generate the Diffie-Helman values,
- run a SHA hash, and
- perform a digital signature.

Such a method requires extensive processing to generate the hashes, the digital signature and the Diffie-Hellman values. It may also present a security risk since the public-private key pair is stored in a non-volatile, potentially accessible memory.

By comparison, the exemplary illustrative non-limiting method disclosed in the present application requires generation of only two random numbers and one public-private key pair, encrypts all data across the wire (except the user ID in one exemplary illustrative non-limiting implementation), requires no pre-sharing or generation of values on the calling party, and has minimal computational impact on the calling party. Such features make it highly advantageous for mobile use.

While the calling party does a huge amount of work in Vanstone, the calling party using the exemplary illustrative non-limiting techniques disclosed herein merely generates a random number, sends it to the called party after encrypting it with the public key received from the called party, and combines it with the second random number received from the called party to generate the shared secret key. This technique is simple, straightforward, secure, and has the potential of being lightning-fast.

Applicant does not understand where the Examiner finds a motivation to combine Vanstone with Bellovin. The Examiner contends it would have been "obvious" to modify Vanstone to exchange the public key in an encrypted message instead of using the public key embedded in Read Only Memory (ROM) and/or obtaining the public key from a trusted third party server. However, it appears that each of Vanstone's "correspondents" needs to have its own PK key pair:

> each of said correspondents C,S having a respective private key e,d and a public key Q_u and Q_s

See col. 1 lines 56-58 (emphasis added). The Examiner wants to modify Vanstone's system by having the correspondents share the same public key which they exchange between themselves. By making such a modification, however, it appears that Vanstone's system would lose the ability to perform other aspects of his method such as for example verifying digital signatures applied by particular devices based on access to a trusted centralized public key database. See e.g., col. 3, line 66 and following ("The hash h will then be used to verify the signature using the public key Q_u recovered from the database. ") Accordingly, such a modification the Examiner is urging is not fairly suggested by the combination of references, and it appears that Vanstone actually teaches away. Such a combination does not render the claimed subject matter obvious. See *KSR International v. Teleflex*, __ U.S. ___, slip opinion at (2007) ("when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be non-obvious.")

There are no passwords in Vanstone's system as required by dependent claim 6, but the Examiner further urges that Vanstone could be modified to use a password. However, because Vanstone's "IDu" is sent to the server in the final step, there is no opportunity for the server to identify the password associated with the calling party to make use of it. Accordingly, such combination is further lacking. Wu does not supply the missing teachings.

Furthermore, applicants believe that the following italicized recitations of independent claim 154, in combination, fully patentably define the claimed subject matter over the prior art of record for the reasons set forth above:

> A method for establishing secure communication between a calling party and a called party, comprising:
>
> generating, on demand at the called party, an asymmetric key pair including a public key and a private key;
>
> *transmitting, from said called party to said calling party, a first encrypted message including a first random number and said public key of said asymmetric key pair*, said called party encrypting said first message with a symmetric encryption key known to the calling party;
>
> said calling party receiving and decrypting said first encrypted message using said symmetric encryption key *to obtain said first random number and said public key*;
>
> said calling party transmitting, to said called party, a second encrypted message including a second random number, *said calling party encrypting said second message with said public key of said asymmetric key pair*;
>
> said called party receiving and decrypting said second encrypted message *to obtain said second random number*;
>
> *said calling and called parties each independently applying said now-shared first and second random numbers to combining functions to thereby each independently generate a shared secret key*; and
>
> said calling and called parties encrypting further communications therebetween *at least in part using said shared secret key*.

All outstanding issues have been addressed and this application is in condition for allowance. Should any minor issues remain outstanding, the Examiner should

contact the undersigned at the telephone number listed below so they can be resolved expeditiously without need of a further written action.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Robert W. Faris/
Robert W. Faris
Reg. No. 31,352

RWF:ejs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100